

89



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/493,984	01/28/2000	Robert S. Eisenbart	18926-003220US	2907

20350 7590 03/02/2005

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER

SIMITOSKI, MICHAEL J

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 03/02/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/493,984

Applicant(s)

EISENBART ET AL.

Examiner

Michael J Simitoski

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 06 December 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,2,4-19 and 21-23 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1,2,4-19 and 21-23 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 28 January 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

1. The RCE with amendments of 12/06/04 was received and considered.
2. Claims 1-2, 4-19 & 21-23 are pending.

Response to Arguments

3. Applicant's arguments with respect to claims 1-2, 4-19 & 21-23 have been considered but are moot in view of the new ground(s) of rejection.
4. Applicant's response (p. 1) requested an interview to discuss any Office Action. Upon contacting applicant's attorney, applicant requested that if any outstanding issues regarding patentability were of a minor nature, they be discussed in a telephone conversation. Upon searching the claims, the Examiner believes the outstanding art is pertinent enough to the case to justify a first action on the merits.
5. Generally commenting on claims 1 & 8, "appending" and "integral" in a network environment can be interpreted differently, depending on the context. For example, in a packet-based network, a packet can only contain so much information. Therefore, appending data larger than a packet to another piece of data and sending it will in fact result in sending the second piece of data "separately" from the first. Similarly, generating a digital signature over a single file and including the signature in the header and sending the file and appended signature, as is well-known in the art, will result in generating a signature over first and second pieces of information (any two parts of the file), appending it to one of the first or second pieces (beginning or end of the file) and sending the signature separately from at least one of the first or the second (different packets).

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 1 & 8 are rejected under 35 U.S.C. 102(b) as being anticipated “How to Sign Digital Streams” by Gennaro et al. (Gennaro). Gennaro discloses generating a signature over first information/hash table and second information/packets, appending the signature to one of the first information or the second information (appended to the hash table), sending the first information/hash table over a network, sending the second information/packets over the network separately from the step of sending the first information/hash table and sending the signature over the network separately from at least one of the first information/hash table or the second information/packets (separate from the second information/packets) (§1.2, ¶3).

8. Claims 1 & 8 are rejected under 35 U.S.C. 102(e) as being anticipated by “Digital Signatures for Flows and Multicasts”, by Wong et al. (Wong).

Regarding claims 1 & 8, Wong discloses generating a signature/block signature ($sign(D_{1-8})$), over first information/first packet (D_1) and second information/second packet (D_2), appending the signature to one of the first information or the second information (appended to each packet), sending the first information/first packet over a network, sending the second information/second packet over the network separately from the step of sending the first

information/first packet and sending the signature/block signature over the network separately from at least one of the first information or the second information (signature is sent with later packets also) (p. 504, §2 (intro) and §A Star Chaining).

Regarding claims 1 & 8, Wong discloses generating a signature/ D_{m-i} over first information/second to last packet and second information/last packet, appending the signature to one of the first information or the second information (appended to second to last packet), sending the first information/second to last packet over a network, sending the second information/last packet over the network separately from the step of sending the first information and sending the signature/ D_{m-i} over the network separately from at least one of the first information or the second information (signature is sent with second to last packet) (p. 503, col. 1, ¶5 – col. 2, ¶2).

9. Claims 1-2, 4-6, 8-9, 11-13 & 21 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent 5,870,474 to Wasilewski et al. (Wasilewski).

Regarding claims 1, 8 & 11, Wasilewski discloses generating a signature/hash over first information/MSK and second information/clear code word (col. 9, lines 31-46), appending the signature/hash to one of the first information or the second information (appended to second information/clear code word) (col. 9, lines 40-46), sending the first information/MSK over a network (col. 11, lines 4-48), sending the second information/clear code word over the network separately from the step of sending the first information (col. 9, lines 40-46) and sending the signature over the network separately from at least one of the first information or the second information (separate from the first information/MSK) (col. 9, lines 31-46 & col. 11, lines 4-48).

Regarding claims 2 & 9, Wasilewski discloses the first information/MSK comprising an authorization data structure/key (col. 9, lines 47-52) and the second information/clear code word comprising a software object/key (col. 9, lines 30-46).

Regarding claim 4, Wasilewski discloses determining which resources a software object in the second information/clear code word is entitled to interact with (which blocks of packets they can decrypt) (col. 8, lines 48-60).

Regarding claim 5, Wasilewski lacks explicitly waiting a predetermined time period after the step of sending the first information before sending the second information. However, it is inherent that, in a packet-based network, a predetermined time period (transmission rate) is waited between each packet, and hence between each piece of information.

Regarding claim 6, Wasilewski discloses the first information/MSK including authorization information for an associated software object/clear code word (col. 9, lines 30-35).

Regarding claim 12, Wasilewski discloses determining a lifetime for which the second information is usable (col. 8, lines 48-60).

Regarding claim 13, Wasilewski discloses checking the first information/MSK for an authorization corresponding to the second information/clear code word (decrypting) (col. 8, lines 25-28).

Regarding claim 21, Wasilewski discloses determining if access of at least one of the first or second information is authorized (determining if control word is authorized) (col. 9, lines 47-58) and ignoring the second information/control word if not authorized (col. 9, lines 47-58).

Art Unit: 2134

10. Claims 7, 10, 14-15 & 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski, as applied to claims 1 and 8 above, in view of U.S. Patent 5,247,364 to Banker et al. (Banker).

Regarding claims 7 & 10, Wasilewski discloses a system, but lacks sending information over different transmission pathways. Banker teaches that unlike in-band transactions, out-of-band subscriber terminals receive data over this channel no matter what the channel the subscriber is tuned to (col. 1, lines 28-44 & col. 2, lines 55-68). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include the first information on a different transmission pathway than the second information. One of ordinary skill in the art would have been motivated to perform such a modification to gain the benefit of delivery regardless of which channel a subscriber was tuned to, as taught by Banker (col. 1, lines 28-44 & col. 2, lines 55-68).

Regarding claim 14, Wasilewski discloses an information object/MSK, authorization information/clear code word wherein a signature/hash is generated over the information object/MSK and the authorization information/clear code word (col. 9, lines 30-38), wherein the signature/hash is integral to one of the information object or the authorization information (integral with the authorization information/ clear code word) (col. 9, lines 40-46). Wasilewski lacks the information object using a first transmission pathway to a set top box, the authorization information using a second transmission pathway to the set top box that is different from the first transmission pathway and the signature using a third transmission pathway to the set top box that is different from at least one of the first or second transmission pathways. However, Banker teaches that unlike in-band transactions, out-of-band subscriber terminals receive data over this

Art Unit: 2134

channel no matter what the channel the subscriber is tuned to (col. 1, lines 28-44 & col. 2, lines 55-68). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include the first information on a different transmission pathway than the second information. One of ordinary skill in the art would have been motivated to perform such a modification to gain the benefit of delivery regardless of which channel a subscriber was tuned to, as taught by Banker (col. 1, lines 28-44 & col. 2, lines 55-68).

Regarding claim 15, Wasilewski discloses an authorization message/ECM, which includes the authorization information/clear code word and the signature (col. 9, lines 40-46).

Regarding claim 19, Wasilewski discloses the information object/MSK sent separately over a network from the authorization information/clear code word (col. 11, lines 10-15).

11. Claims 16 & 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski in view of Banker, as applied to claim 14 above, in further in view of U.S. Patent 6,157,721 to Shear et al. (Shear). Wasilewski discloses a system, as modified above, that uses digital signatures for verification, but is silent regarding multiple signatures. Shear teaches that using several dissimilar digital signatures, via different algorithms, can reduce vulnerability from algorithm compromise (ABSTRACT & col. 7, lines 9-18). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a plurality of signatures with different signing algorithms in Banker's data and to use one or more of the signatures to validate the data. One of ordinary skill in the art would have been motivated to perform such a modification to reduce vulnerability from algorithm compromise, as taught by Shear (ABSTRACT & col. 7, lines 9-18).

12. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski in view of Banker, as applied to claim 14 above, in further in view of U.S. Patent 5,420,866 to Wasilewski (Wasilewski '866). Wasilewski, as modified above, is silent regarding including tiers in the authorization information. However, Wasilewski '866 teaches that satellite and cable access providers include tier information with authorization information sent to decoders to control access to different tiers of programs (col. 4, lines 51-59). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include tier information in the authorization information. One of ordinary skill in the art would have been motivated to perform such a modification to gain the benefit of controlling access to different tiers of programs in a television subscription service, as taught by Wasilewski '866 (col. 4, lines 51-59).

13. Claims 22 & 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski, as applied to claims 1 and 8 above, in view of Shear. Wasilewski discloses a system that uses digital signatures for verification, but is silent regarding multiple signatures. Shear teaches that using several dissimilar digital signatures, via different algorithms, can reduce vulnerability from algorithm compromise (ABSTRACT & col. 7, lines 9-18). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a plurality of signatures with different signing algorithms in Banker's data and to use one or more of the signatures to validate the data. One of ordinary skill in the art would

Art Unit: 2134

have been motivated to perform such a modification to reduce vulnerability from algorithm compromise, as taught by Shear (ABSTRACT & col. 7, lines 9-18).

Conclusion

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. - 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached at (571) 272-3838.

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
Washington, DC 20231

Or faxed to:

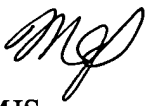
(703)746-7239 (for formal communications intended for entry)

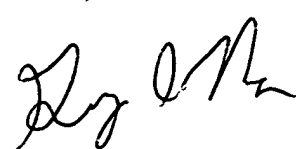
Or:

(571)273-3841 (Examiner's fax, for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


MJS
February 22, 2005


GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100